Шифр гаммирования

Кузьмин Артем

29 мая, 2025, Москва, Россия

Российский Университет Дружбы Народов

Цели и задачи

Цель лабораторной работы

- Освоить на практике применение режима однократного гаммирования на примере кодирования различных исходных текстов одним ключом.

Выполнение лабораторной работы

Гаммирование

Гаммирование – это наложение (снятие) на открытые (зашифрованные) данные криптографической гаммы, т.е. последовательности элементов данных, вырабатываемых с помощью некоторого криптографического алгоритма, для получения зашифрованных (открытых) данных.

Алгоритм взлома

Шифротексты обеих телеграмм можно получить по формулам режима однократного гаммирования:

$$C1 = P1 \oplus K \; C2 = P2 \oplus K$$

Алгоритм взлома

Открытый текст можно найти, зная шифротекст двух телеграмм, зашифрованных одним ключом. Для это оба равенства складываются по модулю 2. Тогда с учётом свойства операции XOR получаем:

$$C1 \oplus C2 = P1 \oplus K \oplus P2 \oplus K = P1 \oplus P2$$

Алгоритм взлома

Предположим, что одна из телеграмм является шаблоном — т.е. имеет текст фиксированный формат, в который вписываются значения полей. Допустим, что злоумышленнику этот формат известен. Тогда он получает достаточно много пар $C1 \oplus C2$ (известен вид обеих шифровок). Тогда зная $P1$ имеем:

$$C1 \oplus C2 \oplus P1 = P1 \oplus P2 \oplus P1 = P2$$

Схема работы алгоритма

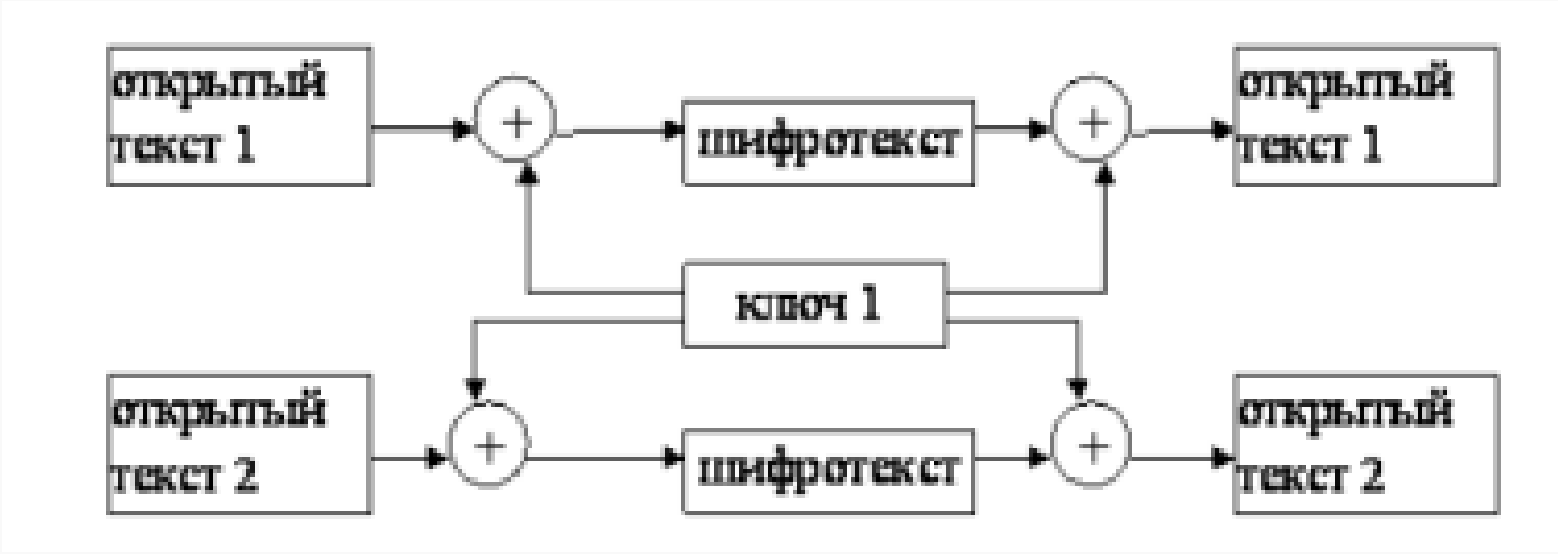

Рис. 1: Работа алгоритма гаммирования

Пример работы программы

```
14 def vzlom(P1, P2):
15     code = []
16     for i in range(len(P1)):
17         code.append(litera[(litera.index(P1[i]) + litera.index(P2[i])) % len(litera)])
18     print(code)
19     pr = "".join(code)
20     print(pr)
```

```
In [11]: 1 len(P1)
Out[11]: 13

In [12]: 1 len(P2)
Out[12]: 13

In [13]: 1 vzlom(P1, P2)
['Х', 'у', 'Л', 'ь', '3', 'а', 'Ж', 'Ф', 'ю', 'с', 'щ', 'ъ', 'Щ']
хулъз3аЖфюсщЩ
```

Рис. 2: Работа алгоритма взлома ключа

Выводы

Результаты выполнения лабораторной работы

В ходе выполнения лабораторной работы было разработано приложение, позволяющее шифровать тексты в режиме однократного гаммирования.